UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/002,697	10/31/2001	Richard Paul Tarquini	10002019-1	4671

7590 11/02/2006

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SON, LINH L D	
ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/002,697	**Applicant(s)** TARQUINI, RICHARD PAUL
	Examiner Linh LD Son	**Art Unit** 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 August 2006*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) □ Notice of Informal Patent Application
6) □ Other: _____.

DETAILED ACTION

1. **This Office Action is responding to the Appeal Brief received on 08/07/06.**

2. **Claims 1-20 are pending.**

3. **Reopening of Prosecution - New Ground of Rejection After Appeal or Examiner's Rebuttal of Reply Brief In view of the Appeal Brief filed on 08/07/06, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below. To avoid abandonment of the application, appellant must exercise one of the following two options: (1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or, (2) request reinstatement of the appeal. If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).**

Claim Rejections - 35 USC § 102

4. **The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:**

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. **Claims 1-6, and 17-18 are rejected under 35 U.S.C. 102(e) as being anticipated by Kloth, US Patent No. 6589034, hereinafter "Kloth".**

6. **As per claims 1 and 17:**

Kloth teaches "A method of identifying data in a network exploit, comprising: receiving a packet by an intrusion prevention system maintained by a node of a network, the intrusion prevention system bound to a media access control driver and a protocol driver " in (Col 4 lines 34-38, Col 7 lines 25-38) [The header information of a packet bound to a media access control driver and a protocol];

> (19) Another example would include a firewall application. For instance, an intruder to a system might be detected, via pattern comparisons and the like established as a function of certain rules. The intruder will have a certain IP address. The intruder's IP stream (or packets) are discarded.
>
> Referring now to FIG. 1, a prior art block diagram 100 is shown of a representative IP flow 102. The IP flow 102 includes a series of data packets 104, 106, and 108 that are interspersed as part of the stream of data. Each IP packet includes certain respective header information 110, 112, and 114. **The headers are used to facilitate sending the packet over a network or the like. The header information is also used by the TCP software to successfully rearrange the packets when they arrive at a destination machine.**

Invoking a signature analysis algorithm by the intrusion prevention system (Col 10 lines 17-25);

> (18) The present invention provides for looking at every part of a packet, with the packet being part of an IP flow coming into the routing engine. **Many different patterns might be defined (via the JIT--or otherwise--compiled rules) for pattern comparison. Once a pattern is detected, a variety of actions might**

7. Claims 1-6, and 17-18 are rejected under 35 U.S.C. 102(e) as being anticipated by Kloth, US Patent No. 6589034, hereinafter "Kloth".

8. As per claims 1 and 17:

Kloth teaches "A method of identifying data in a network exploit, comprising: receiving a packet by an intrusion prevention system maintained by a node of a network, the intrusion prevention system bound to a media access control driver and a protocol driver " in (Col 4 lines 34-38, Col 7 lines 25-38) [The header information of a packet bound to a media access control driver and a protocol];

> (19) Another example would include a firewall application. For instance, an intruder to a system might be detected, via pattern comparisons and the like established as a function of certain rules. The intruder will have a certain IP address. The intruder's IP stream (or packets) are discarded.
>
> Referring now to FIG. 1, a prior art block diagram 100 is shown of a representative IP flow 102. The IP flow 102 includes a series of data packets 104, 106, and 108 that are interspersed as part of the stream of data. Each IP packet includes certain respective header information 110, 112, and 114. **The headers are used to facilitate sending the packet over a network or the like. The header information is also used by the TCP software to successfully rearrange the packets when they arrive at a destination machine.**

Invoking a signature analysis algorithm by the intrusion prevention system (Col 10 lines 17-25);

> (18) The present invention provides for looking at every part of a packet, with the packet being part of an IP flow coming into the routing engine. **Many different patterns might be defined (via the JIT--or otherwise--compiled rules) for pattern comparison. Once a pattern is detected, a variety of actions might be performed.** For instance, a pattern might be changed, modified, or altered. The destination address might be exchanged for another.

utilizing parametric information to select a first rule set from a plurality of rules sets, the first rule set parametrically related to the packet [Parametric information is collected from the TCP, IP, and Application header of the packet, based on the information collected, a set of rules from rules storage 704 is used to define a pattern for analyzing]; and

comparing the packet by the intrusion prevention system with the first rule set comprising a rule logically defining a packet signature" in (See Figure 1, Col 4 lines 38-55 and Col 10 lines 34-49)

> According to one aspect of the present invention, a routing engine is provided that performs a variety of operations. The routing engine will receive and parse an incoming IP flow. For the outset, the engine looks at (or analyzes) all parts of the IP flow, for instance the IP header, TCP header, Application header, etc. The engine then decides whether to forward or buffer the data packet. A set of rules are used to define a pattern (or set of patterns) to be analyzed (or compared/matched) in the incoming IP data flow. The rules can be edited or developed via an appropriate graphical interface. The rules can be applied on-the-fly (e.g. real-time or online, etc.) via a just-in-time (JIT) compiler, or the like. The rules might also be imposed at runtime without the use of a JIT compiler. The pattern can be located anywhere within the IP flow, e.g. IP packet headers or packet data. Upon detection of a certain pattern, actions can be performed upon the IP flow and/or individual IP packets. Such actions can include routing decisions, wherein the packet is mapped to a certain routing capability.
>
> (19) Another example would include a firewall application. For instance, an intruder to a system might be detected, via pattern comparisons and the like established as a function of certain rules. The intruder will have a certain IP address. The intruder's IP stream (or packets) are discarded.
>
> (20) It should be further noted that in parsing the entire IP flow, a virus or the like might be detected in the payload (or other bits) of the IP flow. Relevant infected packets or bit patterns might thereafter be discarded, and/or corrected.
>
> (21) Traffic flow from "spammers" might also be eliminated by detecting the source address pattern of machines sending such undesired information, and thereafter dropping any packets from that source address.

9. As per claim 2:

Kloth teaches "The method according to claim 1, wherein receiving a packet by an intrusion prevention system further comprises receiving a packet originating from the node" in (Col 10 lines 43-46).

> (21) Traffic flow from "spammers" might also be eliminated by detecting the source address pattern of machines sending such undesired information, and thereafter dropping any packets from that source address.

10. As per claim 3:

Kloth teaches "The method according to claim 1, wherein receiving a packet by an intrusion prevention system further comprises receiving a packet originating from a source external to the node, the packet addressed to the node" in (Col 10 lines 43-46).

> (21) Traffic flow from "spammers" might also be eliminated by detecting the source address pattern of machines sending such undesired information, and thereafter dropping any packets from that source address.

11. As per claim 4:

Kloth teaches "The method according to claim 1, further comprising discarding the packet upon determination that a signature of the packet corresponds to the rule" in (Col 4 lines 38-55).

12. As per claim 5:

Kloth teaches "The method according to claim 1, wherein comparing the packet by an intrusion prevention system with a first rule set further comprises comparing the packet by the intrusion prevention system with a second rule set upon determination that a signature of the packet does not correspond to a rule of the first rule set" in (Col 4 lines 38-55).

13. As per claim 6:

Kloth teaches "The method according to claim 1, wherein comparing the packet by the intrusion prevention system with a first rule set further comprises comparing the packet by the intrusion prevention system with a rule set comprising a plurality of rules each respectively comprising machine-readable code logically defining a packet signature" in (Col 4 lines 14-20).

14. As per claim 18:

Kloth teaches "The computer readable medium according to claim 17, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of determining whether a correspondence between a signature of the data packet and the at least one signature files exists" in (See Figure 1, Col 4 lines 38-55)

> According to one aspect of the present invention, a routing engine is provided that performs a variety of operations. The routing engine will receive and parse an incoming IP flow. For the outset, the engine looks at (or analyzes) all parts of the IP flow, for instance the IP header, TCP header, Application header, etc. The engine then decides whether to forward or buffer the data packet. **A set of rules are used to define a pattern (or set of patterns) to be analyzed (or compared/matched) in the incoming IP data flow.** The rules can be edited or developed via an appropriate graphical interface. The rules can be applied on-the-fly (e.g. real-time or online, etc.) via a just-in-time (JIT) compiler, or the like. The rules might also be imposed at runtime without the use of a JIT compiler. **The pattern can be located anywhere within the IP flow, e.g. IP packet headers or packet data.** Upon detection of a certain pattern, actions can be performed upon the IP flow and/or individual IP packets. Such actions can include routing decisions, wherein the packet is mapped to a certain routing capability.

Claim Rejections - 35 USC § 103

15. **The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:**

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

16. **Claims 7-16, and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kloth in view of Vaidya, US Patent No. 6279113 (Cited in 892 dated 03/25/05).**

17. **As per claim 7:**

Kloth teaches "A node of a network maintaining an instance of an intrusion prevention system for identifying data in a network exploit, the node comprising: a central processing unit (Fig 7 #7);

a memory module for storing data in machine-readable format for retrieval and execution by the central processing unit (Fig 6, Memory 604); and

an operating system comprising a network stack comprising a protocol driver, a media access control driver and an instance of the intrusion prevention system bound to the protocol driver and the media access control driver (Col 4 lines 34-38, Col 7 lines 25-38) [The header information of a packet bound to a media access control driver and a protocol], the intrusion prevention system comprising an associative process engine (Col 9 lines 10-24, JIT compiler) and an input/output control layer (Routing engine), the input/output control layer operable to receive a signature file generated from a network exploit rule (Col 10 lines 34-49, The routing engine process the packet according to pattern comparison)

Kloth discloses "the signature file comprising an operand (Col 4 lines 40-45, ie.TCP, IP, and Application header info), an operator (Col 4 lines 19-20, AND/OR...) and a mask (Col 10 lines 44, source or destination address)", but not clearly organized.

Kloth further does not clearly disclose "the input/output control layer operable to pass the signature file to the associative process engine, the associative process engine operable to utilize parametric information to select the signature file from a plurality of signature files, the signature file parametrically related to a data packet, the associative process engine operable to analyze a data packet with the signature file and assign a logical value to the signature file dependent upon a result from the analysis.

Nevertheless, Vaidya discloses the "Dynamic signature Inspection-Based Network Intrusion Detection" invention, which includes a method of associating parametric information to select the signature file from a plurality of signature files, the signature file parametrically related to a data packet, the associative process engine operable to analyze a data packet with the signature file and assign a logical value to the signature file dependent upon a result from the analysis" in (Col 6 lines 1-15, and Col 7 lines 10-30) [The Configuration builder module is the associative process engine. It processes the data collected from the data collector 10 and get the attack signature profiles for the virtual processor to detect the event.] Further Vaidya teaches of "the signature file comprises an operand, an operator, and a mask" in (Col 10 lines 25-45).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Kloth's invention to incorporate Vaidya's teaching of signature file syntax and associating the collected data from the packet to associate with a set of signatures for intrusion prevention. The associates would allows the intrusion prevention system to identified the incoming packets quickly without comparing all the signatures.

18. As per claim 8:

Vaidya teaches "The node according to claim 7, wherein the exploit rule further comprises a composite of a plurality of rules, each rule comprising an operand (), an operator, and a mask having a logical value, each of the plurality of rules being logically connected with at least one of the other plurality of rules by a non-bitwise boolean operator, the logical value of the signature file dependent on the logical value of each of the plurality of rules" in (Col 10 lines 25-45).

19. As per claim 9:

Kloth teaches "The node according to claim 7, wherein the operand comprises network frame data, the operator comprises a bitwise operation, and the mask comprises an operator mask" in (Col 4 lines 15-25).

20. As per claim 10:

Kloth teaches "The node according to claim 7, wherein the network control layer is operable to receive a plurality of signature files each respectively generated from a network exploit rule" in (Col 7 lines 5-10).

21. As per claim 11:

Kloth discloses “The node according to claim 10”, and further discloses a plurality of event patterns for intrusion prevention.

However, Kloth does not specifically ”wherein a parametric association is assigned to a subset of the plurality of signature files, the associative process engine operable to determine a parametric value of the packet and to analyze the packet with the subset of the signature files when the parametric association of the signature files coincide with the parametric value of the packet”

Nevertheless, Vaidya discloses a method of associating parametric information in the IP header to a set of signature profiles in (Col 7 lines 15-30).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Kloth’s teaching to incorporate Vaidya’s disclosure of implementing sets of signatures profile associating to the parametric information from the header of the packet to detect different events of network intrusion for prevention.

22. As per claim 12:

Kloth teaches “The node according to claim 11, wherein the parametric value of the packet is obtained from link-layer header information of the packet” in (Col 4 lines 38-55).

23. As per claim 13:

Kloth teaches "The node according to claim 11, wherein a plurality of parametric associations are respectively assigned to a plurality of subsets of signature files" in (Col 7 lines 15-30).

24. As per claims 14-15 and 19-20:

Kloth teaches "The node according to claim 10". Kloth discloses a method of utilizing a plurality of packet patterns to prevent intrusion.

However, Kloth does not teach "further comprising a table maintained in the memory module, the table comprising a plurality of indices each respectively indexing a subset of the plurality of subsets of signature files and utilizing the subset of signature files for intrusion prevention".

Nevertheless, Vaidya does disclose sets of signature profiles in a memory for intrusion prevention in (Col 6 lines 44-55).

> (7) The configuration generator 28 of the data repository 12 is utilized to establish a configuration of network objects. If more than one data collector 10 is deployed on a network, the configuration generator 28 stores information regarding which objects reside on each segment that a data collector 10 is monitoring and the sets of attack signature profiles required by each data collector. In step 56 the communication module 30 of the data repository 12 distributes the signature profiles to the various data collectors 10 throughout the network. **Upon receiving a set or sets of attack signature profiles, each data collector 10 stores the set or sets of profiles it receives from the data repository 12 in its signature profile memory 39**.

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Kloth's teaching to incorporate Vaidya's disclosure of implementing sets of signatures profile in a database to detect different events of network intrusion for prevention.

25. As per claim 16:

Kloth teaches "The node according to claim 7, However, Kloth does not specifically discloses "wherein the intrusion prevention system further comprises an intrusion event manager, the associative process engine operable to communicate that the analysis of the packet indicates a correspondence with the signature file, the intrusion event manager operable to generate an alert that is transmitted from the node to at least one of a management node in a network and an event database maintained by the node"

Nevertheless, Vaidya discloses a teaching of alerting a network administrator and sending an SMNP message to a monitoring station for storage in (Col 6 lines 20-25).

Therefore, it would have been obvious for one having ordinary skill in the art at the time of the invention was made to modify Kloth's invention to incorporate the SNMP protocol or e-mail alert for caching all events detected.

26. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100